ABSTRACT OF THE DISCLOSURE

Without the need to store and manage a private unique value of a hash function for each token, and without the fear of organizational private information of a center being revealed, a hash function is provided to a token. A unique value input unit is supplied with a unique value d, which is a parameter required to generate a hash function X. A message input unit is supplied with a message M from which to find a hash value. A function generation unique value memory unit 3 holds a function generation unique value s, which is a parameter required to generate a value generation unique value. A value generation unique value calculation unit generates a value generation unique value u from the function generation unique value s and the unique value d. A hash value calculation unit generates a hash value X(M) by applying a hash function H to the value generation unique value u and the message M. A hash value output unit outputs the hash value X(M) generated by the hash value calculation unit.